CIPHERING BETWEEN A CDMA NETWORK AND A GSM NETWORK

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority from U.S. Provisional Patent Application Serial No.60/460,257, filed April 2, 2003.

REFERENCE TO CO-PENDING APPLICATIONS FOR PATENT

[0002] "Internetworking Between A First Network And A Second Network" by Nikhil Jain, having Attorney Docket No. 030259U1, "Authenticating Between A CDMA Network And A GSM Network," by Nikhil Jain, having attorney Docket No. 030259U2, and "Using Shared Secret (SSD) To Authenticate Between A CDMA Network And A GSM Network," by Nikhil Jain, having Attorney Docket No. 030259U3, filed March 18, 2004 and assigned to the assignee hereof, and which are expressly incorporated by reference herein.

FIELD OF THE INVENTION

[0003] The present invention relates generally to wireless communication systems, and more particularly to systems that permit ciphering between a CDMA network and a GSM network.

BACKGROUND

[0004] Code division multiple access (CDMA) is a digital wireless technology that inherently has relatively greater bandwidth capacity, i.e., that inherently permits the servicing of more telephone calls per frequency band, than other wireless communication technologies. Moreover, the spread spectrum principles of CDMA inherently provide secure communications. U.S. Patent No. 4,901,307, incorporated herein by reference, sets forth details of a CDMA system, which can be used to transmit both voice calls and non-voice computer data.

[0005] Despite the advantages of CDMA, other wireless systems exist that use other principles. For example, in much of the world GSM is used, which employs a version of time division multiple access.

[0006] Whether CDMA principles or other wireless principles are used, wireless communication systems can be thought of as having two main components, namely, the wireless radio access network (RAN) and the core infrastructure which communicates with the RAN and with external systems, such as the public switched telephone network (PSTN), the Internet (particularly although not exclusively for data calls), etc. The core infrastructures associated with the various wireless technologies can be very expensive, both in terms of hardware and in terms of developing communication protocols to support particularized, typically system-specific call switching, subscription and attendant authentication and call monitoring, and billing. Consequently, the communication protocols of one wireless system (in the case of GSM, GSM protocols, and in the case of CDMA such as cdma2000-1x, IS-41 protocols) may not be compatible with those of another system without expensively prohibitive alterations in the core infrastructure of one system or the other.

[0007] It would be desirable to internetwork between a CDMA network and a GSM network, thereby enabling the use of a CDMA-based RAN, with its attendant advantages, and enabling the use of a GSM-based core infrastructure, since GSM is extant in much of the world.

[0008] Thus, a dual-mode mobile station may be enabled to advantageously interface with a GSM core infrastructure when in, e.g., Europe, and to use a CDMA infrastructure when in, e.g., the United States.

SUMMARY OF THE INVENTION

[0009] In one aspect of the present invention, a method of wireless communications between a first network and a second network enabling a mobile station (MS) subscribed in the first network to communicate using the second network, comprising storing an identity of the mobile station, obtaining authentication information from the first network based on the identity of the mobile station, using the authentication information from the first network to create a key, substituting the key for SSD-A used in a first algorithm to authenticate the mobile station, and substituting the key for SSD-B used in a second algorithm to encrypt messages between the mobile station and the second network.

[0010] It is understood that other embodiments of the present invention will become readily apparent to those skilled in the art from the following detailed description, wherein various embodiments of the invention are shown and described by way of illustration. As will be realized, the invention is capable of other and different embodiments and its several details are capable of modification in various other respects, all without departing from the spirit and scope of the present invention. Accordingly, the drawings and detailed description are to be regarded as illustrative in nature and not as restrictive.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Figure 1 shows a block diagram of a system architecture using a Mobile Switching Node (MSN) in accordance with an embodiment.

[0012] Figure 2 shows a block diagram of a wireless communications system comprising a CDMA network, a GSM network, General Global Gateway (GGG), and mobile stations in accordance with an embodiment;

[0013] Figures 3a and 3b shows a flowchart for authenticating a CDMA mobile station with a subscription in a GSM network in accordance with an embodiment not using Secret Shared Data (SSD);

[0014] Figure 4 depicts the standard ANSI-41 approach to producing authentication;

[0015] Figure 5 shows the authenticating of a GSM subscriber in an ANSI-41 network using GSM authentication credentials by using Kc as SSD-A in accordance with an embodiment;

[0016] Figure 6 shows the information flow for a successful SSD update procedure in which the GGG updates the SSD shared with the serving MSC/VLR in accordance with an embodiment;

[0017] Figure 7 shows an initial registration scenario modified for SSD sharing in accordance with an embodiment;

[0018] Figure 8 shows the information flow for a successful registration with a new MSC/VLR when SSD sharing is allowed in accordance with an embodiment;

[0019] Figure 9 shows an outline of an authentication procedure for a GSM mobile station in accordance with an embodiment;

[0020] Figure 10 describes GSM key generation with a GSM MS in a GSM network;

[0021] Figure 11 describes CDMA key generation with a CDMA MS in a CDMA network;

[0022] Figure 12 shows a message flow during registration in accordance with an embodiment;

[0023] Figure 13 shows the message flow during a mobile originated (MO) call in accordance with an embodiment; and

[0024] Figure 14 shows the message flow during a mobile terminated (MT) call in accordance with an embodiment.

DETAILED DESCRIPTION

[0025] Acronyms

[0026] 3GPP2 - 3rd Generation Partnership Project 2

[0027] Ack - Acknowledgement

[0028] ACM - Address Complete Message

[0029] ANM - Answer Message

[0030] Assign - Assignment

[0031] AuC - Authentication Center

[0032] Auth – Authentication

[0033] AUTHR – Authentication Response

[0034] BS - Base Station

[0035] BSC - Base Station Controller

[0036] BTS - Base station Transceiver Subsystem

[0037] CAVE - Cellular Authentication and Voice Encryption

[0038] CDMA - Code Division Multiple Access

[0039] CDMA2000 - Third Generation CDMA

[0040] CH - Channel

[0041] CM - Cellular Message

[0042] CMEA - Cellular Message Encryption Algorithm

[0043] ECMEA - Enhanced CMEA

[0044] ESN - Electronic Serial Number

[0045] GSM - Global System for Mobile communications

[0046] GSM1x - Convergence of GSM-MAP with CDMA2000

[0047] HLR - Home Location Register

[0048] IAM - Initial Address Message

[0049] IMSI - International Mobile Subscriber Identity

[0050] ISUP - ISDN User Part

[0051] Info - Information

[0052] IOS - Inter Operability Specification

[0053] IP - Internet Protocol

[0054] Kc - Ciphering Key

[0055] Ki - Individual Subscriber Authentication Key

[0056] MAP - Mobile Application Part

[0057] MIN - Mobile Identification Number

[0058] MO - Mobile Originated

[0059] MS - Mobile Station

[0060] MSN - Mobile Switching Node

[0061] MT - Mobile Terminated

[0062] PDSN - Packet Data Service Node

[0063] PLC - Private Long Code

[0064] PLCM - PLC Mask

[0065] Priv - Privacy

[0066] PSTN - Public Switched Telephone Network

[0067] RAN - Radio Access Network

[0068] RAND - Random Challenge Data

[0069] Req - Request

[0070] Resp - Response

[0071] SIM - Subscriber Identity Module

[0072] SMS - Short Message Service

[0073] SMSC - Short Message Service Center

[0074] SRES – Signed Response

[0075] SSD - Shared Secret Data

[0076] SS7 - Signaling System 7

[0077] TCH – Traffic Channel

[0078] VP - Voice Privacy

[0079] VPM - VP Mask

[0080] System Architectures

[0081] In an embodiment, the system integrates a CDMA RAN with a GSM Core network. This is achieved by using a mobile station (MS) with a GSM subscription and a GSM network entity. Two of the options for the GSM network entity are:

(1) A Mobile Switching Node (MSN); and

(2) An Interworking and Interoperability Function (IIF).

[0082] A Mobile Switching Node (MSN) is a network switching element that supports communication between a standard IOS compliant CDMA RAN and a GSM Core network. The GSM MSN will work with GSM Core network entities such as the HLR, AuC and SMSC. The GSM system architecture using the MSN is shown in Figure 1.

[0083] A General Global Gateway (GGG) is an Interworking and Interoperability Function (IIF) that interworks between the CDMA and GSM core networks. The term, "interworks," and "internetworks," can be interchanged. In an embodiment, the GGG can be called a GSM1x Global Gateway. The GGG represents an evolution to the J-STD-038 IIF that enhances authentication and SMS functionality. This GGG solution uses a standard CDMA MSC/VLR in addition to a CDMA RAN. The GGG interworks between these elements and the standard GSM network elements such as HLR, AuC, GMSC and SMSC. The GSM system architecture using the GGG is shown in Figure 2.

MSN Architecture

[0084] Figure 1 shows a block diagram of a system architecture 100 using an MSN in accordance with an embodiment. The system 100 comprises mobile stations 102, a CDMA network 104, a GSM network 106, an MSN 108, a PDSN 110, an IP network 112, and PSTN 114.

[0085] The CDMA network 104 comprises BTSs and BSCs. The CDMA network 104 interfaces with a PDSN 110, which interfaces with an IP network 112. In an embodiment, the interface between the CDMA network 104 and the PDSN 110 is according to IOS 4.x. In an embodiment, the interface between the PDSN 110 and the IP network 112 uses an IP.

[0086] The CDMA network 104 interfaces with a GSM MSN 108. In an embodiment, the interface between the CDMA network 104 and the GSM MSN 108 is according to IOS 4.x.

[0087] The GSM MSN 108 interfaces to a PSTN 114. In an embodiment, the interface between the GSM MSN 108 and the PSTN 114 is via ISUP.

[0088] The GSM MSN 108 interfaces to the GSM network 14. In an embodiment, the GSM network 14 comprises a GSM SS7 116, a GSM Short Message Center (GSM SMSC) 118, a GSM Home Location Register (GSM HLR) 120, and a GSM Authentication Center (GSM AuC) 122.

GGG Architecture

[0089] Figure 2 shows a block diagram of a wireless communications system 10 comprising a CDMA network 12, a GSM network 14, General Global Gateway (GGG) 16, and mobile stations 18, 20, 22, 24 in accordance with an embodiment. GSM mobile station 20 includes a Subscriber Identity Module (SIM) 26. CDMA mobile station 24 includes SIM 28. SIMs 26, 28 are removable engaged with mobile stations 20, 24, respectively, in accordance with principles known in the art. In an embodiment, the GGG is a GSM Global Gateway.

[0090] The GGG 16 internetworks between the CDMA network 12 and the GSM network 14. The GGG includes a transceiver (not shown) that allows it to send and receive messages to and from the CDMA network 12 and the GSM network 14.

[0091] In an embodiment, the CDMA network is an ANSI-41 network. It would be apparent to those skilled in the art, the CDMA network 12 may be any variety of CDMA networks including, but not limited to cdma2000-1x and cdma2000-1xEV-DO. It would also be apparent to those skilled in the art, the GSM network 14 may be any variety of GSM network or successor network including, but not limited to General Packet Radio Services (GPRS), Universal Mobile Telecommunication System (UMTS), and Wideband-CDMA (W-CDMA).

[0092] The GSM network 14 comprises a GSM Core 30 and a GSM Radio Access Network 32. The GSM Core 30 comprises a GSM Home Location Register (GSM HLR) 34, a GSM Authentication Center (GSM AuC) 36, a GSM Short Message Center (GSM SMSC) 38 and a GSM Gateway Mobile Switching Center (GSM GMSC) 40. The CDMA network 12 comprises a a CDMA Home Location Register (CDMA HLR) 42, a CDMA Authentication Center (CDMA AuC) 44, CDMA MSC 46 and associated CDMA Radio Access Network (CDMA RAN) 48.

[0093] With respect to a GSM mobile station with a subscription in a CDMA Core 20, the GGG 16 functions as a Visitor Location Register (VLR) 50 to the GSM network 14. With respect to a CDMA mobile station 24 with a subscription in a GSM Core 30, the GGG 16 functions as a Visitor Location Register (Visitor LR) 52 to the CDMA network 12.

[0094] Mobile stations 18, 20, 22, 24 do not need to have a subscription in both core infrastructures 12, 14 and may have a subscription in only one of the core infrastructures 12, 14.

[0095] With respect to both the GSM mobile station with a subscription in a CDMA Core 20 and a CDMA mobile station with a subscription in a GSM Core 24, the GGG 16 functions as a Short Message Service Center (SMSC) 54. It would be apparent to those skilled in the art that the GGG 16 can include or communicate with the SMSC 54.

[0096] Mobile stations 18, 20 support a GSM signaling protocol, a GSM Authentication procedure, and a GSM Short Message Service. Likewise, mobile stations 22, 24 support a CDMA signaling protocol, a CDMA Authentication procedure, and a CDMA Short Message Service.

[0097] During registration of a CDMA mobile station with a subscription in the GSM core 24, the GGG acts as an Authentication Controller in a CDMA network, but authenticates the mobile station 24 using the GSM authentication mechanism. Likewise, during registration of a GSM mobile station with a subscription in the CDMA core 20, the GGG acts as an Authentication Controller in a GSM network, but authenticates the mobile station 20 using the CDMA authentication mechanism.

[0098] The GGG acts as a message center via Short Message Service Center 54. In a CDMA network, SMS messages are routed to and from the mobile station 24 using a CDMA SMS mechanism. In other words, in a CDMA network, GSM messages are tunneled to and from mobile station 24 using a CDMA SMS mechanism. The GSM messages are encapsulated within CDMA SMS messages.

[0099] Likewise, in a GSM network, SMS messages are routed to and from the mobile station 20 using a GSM SMS mechanism. In other words, in a GSSM network, CDMA messages are tunneled to and from mobile station 20 using a GSM SMS mechanism. The CDMA messages are encapsulated within GSM SMS messages.

[00100] An incoming call to a registered GSM subscriber 24 arrives at GSM gateway MSC (GSM GMSC) 40 in the subscriber's home GSM network 14. The GMSC 40 interrogates the GSM LR 50 to determine the location of the subscriber 24, which is in the CDMA network 12. The location of the GSM subscriber 24 from the perspective of the GSM LR 50 is in the GGG 16, which appears as a GSM VLR. When the GSM LR 50 requests routing information from the GGG 16, the GGG 16 requests routing information from the serving CDMA LR 52 and thus the call is routed to the CDMA MSC 46.

[00101] Likewise, an incoming call to a registered CDMA subscriber 20 arrives at CDMA MSC 46 in the subscriber's home CDMA network 12. The CDMA MSC 46 interrogates the CDMA LR 52 to determine the location of the subscriber 20, which is in the GSM network 14. The location of the CDMA subscriber 20 from the perspective of the CDMA LR 52 is in the GGG 16, which appears as a CDMA VLR. When the CDMA LR 50 requests routing information from the GGG 16, the GGG 16 requests routing information from the serving GSM LR 50 and thus the call is routed to the GSM GMSC 40.

[00102] The CDMA-based mobiles stations 22, 24 communicate with a CDMA mobile switching center (MSC) 46 using a CDMA radio access network (RAN) 48 in accordance with CDMA principles known in the art. In an embodiment, the CDMA MSC 46 is an IS-41 MSC.

[00103] Likewise, the GSM-based mobiles stations 18, 20 communicate with a GSM mobile switching center (GSM GMSC) 40 using a GSM RAN 32 in accordance with GSM principles known in the art.

[00104] In accordance with CDMA principles known in the art, the CDMA RAN 48 includes base stations and base station controllers. In an embodiment, CDMA RAN 24 shown in Figure 2 uses cdma2000, and specifically uses either cdma2000 1x, cdma2000 3x, or cdma2000 high data rate (HDR) principles.

[00105] In accordance with GSM principles known in the art, the GSM RAN 32 includes base stations and base station controllers. In an embodiment, GSM RAN 32 uses either GSM, GPRS, EDGE, UMTS, or W-CDMA principles.

[00106] The CDMA core infrastructure comprising the CDMA MSC 46 and CDMA RAN 48 can include or can access a CDMA authentication center (CDMA AUC) 44 and a CDMA home location register (CDMA HLR) 42 in accordance with CDMA principles known in the art to authenticate subscriber mobile station 22, and to collect accounting and billing information as required by the particular CDMA core infrastructure.

[00107] Likewise, the GSM core 30 can include or can access a GSM authentication center (GSM AUC) 36 and a GSM home location register (GSM HLR) 34 in accordance with GSM principles known in the art to authenticate subscriber mobile station 18, and to collect accounting and billing information as required by the particular GSM core infrastructure.

[00108] The CDMA MSC 46 uses the GGG 16 to communicate with the GSM network 14. The GSM network 14 can include or can access a GSM authentication center 36 and a

GSM home location register (HLR) 34 in accordance with GSM principles known in the art to authenticate subscriber mobile station 24 and to collect accounting and billing information as required by the particular GSM core 30.

[00109] Likewise, GSM GMSC 40 uses the GGG 16 to communicate with the CDMA network 12. The CDMA network 12 can include or can access a CDMA authentication center 44 and a CDMA home location register (HLR) 42 in accordance with CDMA principles known in the art to authenticate subscriber mobile station 20 and to collect accounting and billing information as required by the particular CDMA network 12.

[00110] Both the GSM core 30 and the CDMA core infrastructure can communicate with a network such as a public switched telephone network (PSTN) and/or an Internet Protocol (IP) network.

[00111] With respect to a CDMA mobile station 24 with a subscription in a GSM Core 30, the GGG 16 functions as a VLR 50 to the GSM network 14. The GGG meets GSM protocol requirements for a VLR 50. The GGG interacts with GSM core network elements such as GSM HLR 34 and GSM SMSC 38 according to GSM specifications, except that the GGG 16 routes incoming calls to the CDMA network 12. The GSM LR 50 also performs a location update with the GSM network 14 when the mobile station registers in the CDMA network 12. In this sense, the GGG acts as a VLR to the whole CDMA network 12.

[00112] With respect to a GSM mobile station 20 with a subscription in a CDMA network 12, the GGG 16 functions as a VLR 52 to the CDMA network 14. The GGG meets CDMA protocol requirements for a VLR 52. The GGG interacts with CDMA core network elements such as CDMA HLR 42 and CDMA MSC 46 according to CDMA specifications, except that the GGG 16 routes incoming calls to the CDMA network 12. The CDMA LR 52 also performs a location update with the CDMA network 12 when the mobile station registers in the GSM network 14. In this sense, the GGG acts as a VLR to the whole GSM network 14.

[00113] When a mobile station that is in the CDMA network 12 is called from the GSM network 14, the call is routed to the CDMA LR 52 in the GGG 16 per standard specifications. The GGG 16 routes the call to the CDMA network 12. The CDMA network 12 eventually routes the call to the CDMA MSC 46 serving the mobile station. Similarly, if an SMS is routed to the CDMA network 12 from the GSM network 14, the GGG 16 routes the message to a message center (not shown) within the CDMA network 12.

[00114] When a mobile station that is in the GSM network 14 is called from the CDMA network 12, the call is routed to the GSM LR 50 in the GGG 16 per standard specifications. The GGG 16 routes the call to the GSM network 14. The GSM network 14 eventually routes the call to the GSM GMSC 40 serving the mobile station. Similarly, if an SMS is routed to the GSM network 10 from the CDMA network 12, the GGG 16 routes the message to a GSM SMSC 38 within the GSM network 14.

[00115] When a mobile station registers with the CDMA network 12, the CDMA network 12 sends a location update indication to the GSM network 14. The GSM LR 50 then performs a location update as per standard specifications with the GSM core network 14.

[00116] When a mobile station registers with the GSM network 14, the GSM network 14 sends a location update indication to the CDMA network 12. The CDMA LR 52 then performs a location update as per standard specifications with the CDMA network 12.

[00117] With respect to a CDMA mobile station 24 with a subscription in a GSM Core 30, the GGG 16 acts as an HLR 52 in the CDMA network 12. The CDMA LR 52 shall meet HLR protocol requirements for GSM to CDMA roaming. An important piece of information that the HLR 50 maintains is the address of the CDMA MSC 46 serving the mobile station 24. When the GSM LR 50 in the GGG 16 routes a call to the CDMA side 12, the CDMA LR 52 will further route it to the serving MSC 46.

[00118] With respect to a GSM mobile station 20 with a subscription in a CDMA network 12, the GGG 16 acts as an HLR 50 in the GSM network 14. The GSM LR 50 shall meet HLR protocol requirements for CDMA to GSM roaming. An important piece of information that the HLR maintains is the address of the GSM GMSC 40 serving the mobile station 20. When the CDMA LR 52 in the GGG 16 routes a call to the GSM side 14, the GSM LR 50 will further route it to the serving MSC 40.

[00119] The GGG acts as an Authentication Controller (AUC) in the CDMA network for GSM subscribers 24. The AUC 44 in a CDMA network 12 is responsible for authenticating a mobile station and permitting/denying access to network resources. The AUC function in the GGG does not call for A-key provisioning at the GGG or the MS. Instead the GGG uses the GSM authentication credentials and the GSM authentication method via GSM signaling to authenticate the mobile station 24. The GGG responds to valid messages that can be received by a CDMA AUC 44.

[00120] The GGG acts as an Authentication Controller (AUC) in the GSM network for CDMA subscribers 20. The AUC 36 in a CDMA network 14 is responsible for

authenticating a mobile station and permitting/denying access to network resources. The AUC function in the GGG does not call for A-key provisioning at the GGG or the MS. Instead the GGG uses the CDMA authentication credentials and the CDMA authentication method via CDMA signaling to authenticate the mobile station 20. The GGG responds to valid messages that can be received by a GSM AUC 36.

[00121] The GGG 16 acts as a Message Center (MC) in the CDMA network 12 and routes SMS messages between the CDMA mobile station 24 and GSM GMSC 40 using a GSM SMS mechanism.

[00122] Likewise, the GGG 16 acts as a Message Center (MC) in the GSM network 14 and routes SMS messages between the GSM mobile station 20 and CDMA MSC 46 using a CDMA SMS mechanism.

[00123] The CDMA MS 24 is required to have a valid identity in the CDMA network. If this identity is different from the GSM International Mobile Subscriber Identity (IMSI) (i.e., if the CDMA network does not use true IMSI), then the GGG provides a mapping between the CDMA identity and the GSM IMSI. It would be apparent to those skilled in the art that any technique/method known in the art to uniquely identify the mobile station 24 may be used.

[00124] The GSM MS 20 is required to have a valid identity in the GSM network. In an embodiment, this identity is a GSM IMSI (i.e., if the CDMA network does not use true IMSI). If the identity in the GSM network is different from the identity in a CDMA network, then the GGG provides a mapping between the GSM identity and the CDMA identity. It would be apparent to those skilled in the art that any technique/method known in the art to uniquely identify the mobile station 20 may be used.

[00125] In a non-limiting embodiment, mobile stations 18, 20, are mobile telephones made by Kyocera, Samsung, or other manufacturer that use GSM principles and GSM over-the-air (OTA) communication air interfaces. In a non-limiting embodiment, mobile stations 22, 24, are mobile telephones made by Kyocera, Samsung, or other manufacturer that use CDMA principles and CDMA over-the-air (OTA) communication air interfaces. The present invention, however, applies to other mobile stations such as laptop computers, wireless handsets or telephones, data transceivers, or paging and position determination receivers. The mobile stations can be hand-held or portable as in vehicle-mounted (including cars, trucks, boats, planes, trains), as desired. However, while wireless communication devices are generally viewed as being mobile, it is to be understood that

the present invention can be applied to "fixed" units in some implementations. Also, the present invention applies to data modules or modems used to transfer voice and/or data information including digitized video information, and may communicate with other devices using wired or wireless links. Further, commands might be used to cause modems or modules to work in a predetermined coordinated or associated manner to transfer information over multiple communication channels. Wireless communication devices are also sometimes referred to as user terminals, mobile stations, mobile units, subscriber units, mobile radios or radiotelephones, wireless units, or simply as "users" and "mobiles" in some communication systems.

Authentication without using SSD

[00126] Figures 3a and 3b shows a flowchart for authenticating a CDMA mobile station 24 with a subscription in a GSM network 14 in accordance with an embodiment not using SSD. Figures 3a and 3b are described as they inform the description of Figure 6.

[00127] In step 202, mobile station 24 (MS) roams into a CDMA area and the flow of control proceeds to step 204. In step 204, the mobile station 24 initiates a registration system access to a CDMA MSC 46 via a CDMA RAN 48 and the flow of control proceeds to step 206.

[00128] The registration system access is a message to the CDMA MSC 46 via the CDMA RAN 48, the message including an identity of the mobile station 24. In an embodiment, the identity of the mobile station 24 may be provided by the SIM 28. In an embodiment, the identity of the mobile station 24 is an IMSI. In an embodiment, the identity of the mobile station 24 is a Mobile Identification Number (MIN).

[00129] In step 206, the CDMA MSC 46 determines, based on the mobile station identity, whether the mobile station 24 is a GSM subscriber. In an embodiment, wherein the identity of the mobile station 24 is an IMSI, the MSC 46 can make this determination because the IMSI contains, among other information, a code representing the country and network in which the mobile station has a subscription.

[00130] In the event that the CDMA-subscribing mobile station 22 is the mobile station under test, the flow of control proceeds to step 208. In step 208, the mobile station 22 is authenticated using CDMA principles by the CDMA core infrastructure, using the CDMA HLR 42 and CDMA AUC 44.

[00131] In the event that the CDMA mobile station 24 with a subscription in the GSM network 14 is the mobile station under test, the flow of control proceeds to step 210. In step 210, the CDMA MSC 46 accesses the GGG 16 by sending an Authentication Request to the CDMA LR 52 in the GGG 16 and the flow of control proceeds to step 212 in accordance with an embodiment. In another embodiment, the flow of control proceeds to step 214.

[00132] In an embodiment, the identity of the mobile station 24 is sent to the CDMA LR 52 as part of the Authentication Request. Alternatively, the identity of the mobile station 24 is sent to the CDMA LR 52 in addition to the Authentication Request.

[00133] In an embodiment, the Authentication Request may include parameters MIN, ESN and COUNT. ESN is an electronic serial number.

[00134] In an embodiment, the Authentication Request may include parameters MIN, ESN and COUNT. ESN is an electronic serial number. COUNT represents a count of a predetermined event that is a mutually agreed upon event between the GGG 16 and mobile station 24. In an embodiment, the GGG 16 shares the updating of COUNT with a node that interacts with the GGG 16. By sharing the update function with another node, the message traffic between the GGG 16 and the other node may be reduced. For example, if the GGG 16 shares the function of updating COUNT with the CDMA MSC 46, then the message traffic between the GGG 16 and the CDMA MSC 46 may be reduced.

[00135] In an embodiment, COUNT represents the number of times a mobile station 24 attempts to access the GSM network 14. Each time the mobile station 24 accesses the GSM network, the GGG updates a COUNT for the particular mobile station 24. The mobile station 24 also updates its own COUNT for the number of times it accesses the GSM network 14. The GGG 16 stores the value of the ESN. In another embodiment, COUNT represents a number of requests for authentication by the mobile station. It would be apparent to those skilled in the art that there are many events that can be counted, which the mobile station 24 and GGG 16 can count.

[00136] In step 212, the GGG 16 compares the value of COUNT to a count value in a GGG database. If the value of COUNT is equal to the count value in the GGG database, then the flow of control proceeds to step 214. If the value of COUNT is not equal to the count value in the GGG database, then the flow of control proceeds to step 216. It would be

apparent to those skilled in the art that depending on an application, a variety of criteria may be applied to determine whether an Authentication Request is honored.

[00137] In step 214, an Authentication Request Return Result (ARRR) is set to true and the flow of control proceeds to step 218. The Authentication Request Return Result message indicates the result of the Authentication Request.

[00138] In step 216, the Authentication Request Return Result is set to false and the flow of control proceeds to step 220.

[00139] In response to the Authentication Request Return Result being true, the GGG 16 accesses the GSM network 14 and obtains necessary authentication information from the GSM HLR 34 and GSM AuC 36. In step 218, the GGG 16 looks up the MIN in its database to obtain a corresponding GSM IMSI and accesses the GSM network 14 by sending a GSM HLR authentication message with the IMSI of the mobile station 24 to the GSM HLR/AuC 34, 36, in accordance with an embodiment. The flow of control proceeds to step 220.

[00140] Method steps can be interchanged without departing from the scope of the invention. Thus, it would be apparent to those skilled in the art that step 218 does not have to be performed before step 220.

[00141] In step 220, the GGG 16 sends the Authentication Request Return Result to the CDMA MSC 46 and the flow of control proceeds to step 222. In step 222, the Authentication Request Return Result is tested. If the Authentication Request Return Result is true, then in step 224 the GGG 16 starts a timer, T_{REG} and the flow of control proceeds to step 226.

[00142] If the Authentication Request Return Result is false, then the flow of control proceeds to step 228. In step 228, the CDMA MSC 46 sends a mobile station authentication message to the mobile station 24 indicating the mobile station 24 is not authenticated. It would be apparent to those skilled in the art that the mobile station may reattempt authentication depending on the application.

[00143] The GGG includes a logic unit (not shown) to execute program logic. It would be apparent to those skilled in the art that the logic unit may include a general purpose processor, a special-purpose processor, and/or firmware.

[00144] In step 226, the CDMA MSC 46 upon receiving an Authentication Request Return Result indicating successful authentication, sends a Registration Notification to the CDMA LR 52 in the GGG 16. The flow of control proceeds to step 230.

[00145] In step 230, a check is made to determine whether the GGG 16 received the Registration Notification before T_{REG} expired. If the GGG 16 received the Registration Notification before T_{REG} expired, then the flow of control proceeds to step 232, otherwise the flow of control proceeds to step 234. In step 232, Registration Notification Return Result is set to indicate T_{REG} did not expire and the flow of control proceeds to step 236. In step 234, Registration Notification Return Result is set to indicate T_{REG} expired and the flow of control proceeds to step 236.

[00146] In step 236, the GGG 16 responds to the Registration Notification with a Registration Notification Return Result indicating whether T_{REG} expired. The Registration Notification Return Result is sent from the GGG 16 to the CDMA MSC 46.

[00147] In an embodiment, the GGG 16 sends a message with or within the Registration Notification Return Result indicating SMS only mode/status. "SMS only" means the mobile station 24 sends and receives only SMS messages, not data and/or voice messages. The flow of control proceeds to step 238.

[00148] In step 238, the CDMA MSC 46 sends a Registration Accept message to the mobile station 24 upon receiving the Registration Notification Return Result. Like the Registration Notification Return Result, the Registration Accept message indicates whether T_{REG} expired. The flow of control proceeds to step 240.

[00149] In step 240, the mobile station 24 determines whether the Registration Accept message indicates an accepted registration, i.e., T_{REG} did not expire. If T_{REG} expired, then the flow of control proceeds to step 242, otherwise the flow of control proceeds to step 244.

[00150] In step 242, the mobile station 24 may or may not reattempt registration. It would be apparent to those skilled in the art that depending on a mobile station application, the mobile station may or may not reattempt registration.

[00151] Method steps can be interchanged without departing from the scope of the invention. Thus, it would be apparent to those skilled in the art that step 244 does not have to be performed after step 242.

[00152] Step 244 only has to be executed after the GSM HLR authentication message has been sent to the GSM HLR/AuC 34, 36 of step 218. In step 244, the GSM HLR/AuC 34, 36 sends a GGG authentication message including authentication parameters to the GGG 16 and the flow of control proceeds to step 246.

[00153] After the GGG 16 successfully sends the Registration Notification Return Result to the CDMA MSC 46 and receives the GGG authentication message from the GSM HLR/AuC 34, 36, the GGG 16 sends a GSM authentication request message to the CDMA MSC 46 in step 246. The flow of control proceeds to step 248. In step 248, the CDMA MSC 46 forwards the GSM authentication request message to the mobile station 24 and the flow of control proceeds to step 250.

[00154] In an embodiment, an application may have more criteria for authenticating mobile stations apart from the criteria applied to the original Authentication Request of step 210. Thus, in an embodiment, the CDMA MSC 46 sends a second authentication request (not shown) to the GGG 16 and the GGG 16 responds to the second authentication request (not shown).

[00155] In step 250, the mobile station 24 responds to the GSM authentication request message by determining authentication parameters such as an encryption key using a GSM authentication method and sending an authentication response including the authentication parameters to the CDMA MSC 46. In an embodiment, the authentication response is sent using the IS-637 SMS transport. The flow of control proceeds to step 252.

[00156] In step 252, the CDMA MSC 46 forwards the authentication response to the GGG 16 and the GGG 16 validates that the authentication parameters by matching the authentication parameters to values received from the GSM HLR/AuC 34, 36 in step 244. The flow of control proceeds to step 254.

[00157] In step 254, the GGG 16 sends an update location message to the GSM HLR 34 to update the location of the mobile station 24 and the flow of control proceeds to step 256. In step 256, the GSM HLR 34 sends GSM subscriber profile data of the mobile station 24 to the GSM LR 50 in the GGG 16. The flow of control proceeds to step 258.

[00158] In step 258, the GGG 16 maps the GSM subscriber profile data to a CDMA subscriber profile and sends the CMDA profile data in a Qualification Directive to the CDMA MSC 46 and the flow of control proceeds to step 260. The Qualification Directive indicates that the mobile station 24 is qualified, i.e., authorized to communicate with the GSM network 14. If the mobile station 24 is not qualified, then mobile station 24 is not authorized to communicate with the GSM network 14 (not shown). In an embodiment, the GGG 16 indicates to the CDMA MSC 46 "full profile," which in turn is forwarded to

the mobile station 24 and indicates to the mobile station 24 that the mobile station 24 can send and receive without being limited to SMS messages.

[00159] In step 260, the CDMA MSC 46 responds to the Qualification Directive and sends a Qualification Directive Response to the CDMA LR 52 and the flow of control proceeds to step 262.

[00160] In step 262, responsive to the GSM LR 50 receiving the GSM subscriber profile data, the GGG 16 sends a GSM subscriber profile data response to the GSM HLR/AuC 34, 36.

[00161] In step 264, responsive to the GSM HLR 34 receiving the update location message from the GGG 16 in step 254, the GSM HLR 34 responds to the update location message and sends a update location message response to the GSM LR 50, the update location message response indicating that the location of the mobile station 24 has been updated at the GSM LR 50.

Authentication Keys

[00162] It is in the area of authentication that the GGG differs most from the J-STD-038 IIF. Since the J-STD-038 IIF requires that the roaming subscriber have dual subscriptions – one for ANSI-41 and the other for GSM – it uses standard ANSI-41 techniques to authenticate the subscriber in ANSI-41 foreign mode. In contrast, the GGG solution does not require that the ANSI-41 foreign mode roamer have a complete ANSI-41 subscription. In particular, either the MS or GGG needs to be provisioned with ANSI-41 A-keys. The following first describes the standard ANSI-41 authentication mechanism. Then modifications to ANSI-41 method are described.

Standard ANSI-41 Authentication

[00163] The standard ANSI-41 approach to producing authentication keys is depicted in Figure 4. The A-key (which is the secret data known only to the mobile station and authentication center) and a random number called RANDSSD are processed using a CAVE algorithm to produce a 128-bit number called the Secret Shared Data (SSD). This operation is performed in the mobile station and the authentication center. The SSD consists of a 64-bit SSD-A key used for authentication and a 64-bit SSD-B key used for encryption. On each system access the mobile station generates an authentication response (AUTHR) by processing SSD-A, ESN, MIN, authentication data

(AUTH_DATA – either IMSI_S or dialed digits depending on the system access type) and a random number (RAND) broadcast by the RAN in overhead messages. The processing is performed again by executing the CAVE algorithm. The mobile station transmits AUTHR in the system access and is authenticated when the authentication center (or optionally the MSC/VLR) independently performs the same computation and compares the result with that received.

Using Kc as SSD-A

[00164] The goal of authenticating a GSM subscriber in an ANSI-41 network using the GSM authentication credentials can be achieved by using Kc as SSD-A. The new method to generate the SSD-A key and AUTHR in accordance with an embodiment is shown in Figure 5. When the GSM authentication is run at the mobile station and at the GSM AuC, the secret key Ki (known only to the subscriber's SIM and the GSM AuC) and the random number (GSM_RAND) are used to produce the SRES and the encryption key Kc.. Kc is 64 bits in length just as SSD-A. Therefore, Kc can be substituted for the SSD-A value in the standard ANSI-41 computation of AUTHR using a CAVE algorithm.

[00165] Since the GGG gets the GSM authentication triplets (i.e., GSM_RAND, SRES and Kc) from the GSM AuC and the RAND, ESN, MIN and AUTH_DATA in an AuthenticationRequest INVOKE it can then use the Kc value as the SSD-A value to authenticate the mobile station using the ANSI-41 method after the mobile station is first authenticated using GSM_RAND. In other words, the GGG and the mobile station have a common value of Kc after the mobile station executes the GSM authentication procedure using the value of GSM_RAND at the GGG. This GSM authentication can be performed in the ANSI-41/CDMA2000 network using GSM signaling over IS-637 SMS transport. Once the mobile station and GGG have the same value of Kc, then this value can be used as SSD-A and standard ANSI-41 methods can be used to authenticate the mobile station. The advantage of using the ANSI-41 authentication techniques is better signaling efficiency. Note that this approach also meets the goal of authenticating a mobile station in the ANSI-41 network using GSM credentials.

Authentication with SSD sharing

[00166] For the operational scenario of Figure 3, the ANSI-41 AC in the GGG retains authentication responsibility. The serving MSC/VLR is assumed to respond to each

mobile station access attempt (e.g., registration, origination, page response and flash) with an AuthenticationRequest INVOKE towards the ANSI-41 HLR/AC in the GGG. While this approach provides maximum security, the tradeoff is more signaling traffic between the ANSI-41 MSC/VLR and the GGG.

[00167] To reduce MSC/VLR – HLR/AC signaling traffic, a method that allows the AC to distribute some authentication responsibility with the serving MSC/VLR is described below. SSD sharing is applied to a GGG-based GSM1x solution if the value of Kc is used for SSD-A as described in reference to Figure 4. The remainder of this section describes how SSD sharing is performed.

SSD update

[00168] Figure 6 shows the information flow for a successful SSD update procedure in which the GGG updates the SSD shared with the serving MSC/VLR in accordance with an embodiment. The initial condition for this scenario is that the GGG has previously shared SSD with the serving MSC/VLR and that the MSC/VLR authenticates the MS when it performs a system access.

[00169] The following procedure describes this information flow:

[00170] In step 501, the GGG initiates the SSD update by invoking Authentication Directive (IS41_AUTHDIR) towards the ANSI-41 MSC/VLR with the MIN, ESN and NOSSD parameters.

[00171] In step 502, the MSC/VLR discards the SSD that it has for the specified MS, and responds by invoking Authentication Directive Return Request towards the GGG. The MSC/VLR will now invoke Authentication Request towards the HLR/AC in the GGG for each system access of this MS.

[00172] In step 503, the GGG invokes Count Request (IS41_COUNTREQ) towards the MSC/VLR to request the current value of the CallHistoryCount (COUNT) parameter for the MS.

[00173] In step 504, the MSC/VLR responds with the Count Request Return Result (IS41_countreq), containing the requested COUNT parameter.

[00174] In step 505, if the GGG has no additional GSM authentication triplets for the MS, then the GGG invokes MAP_SEND_AUTHENTICATION_INFO towards the GSM HLR. The next time that the MS accesses the system, the following steps occur:

[00175] In step 506, the GSM HLR responds with MAP_send_authentication_info containing a set (at least one) of authentication triplets.

[00176] In step 507, the next time the MS accesses the system, the following occurs:

[00177] In step 508, since SSD is no longer being shared, the MSC/VLR invokes Authentication Request (IS41_AUTHREQ) towards the GGG to authenticate the MS system access.

[00178] In step 509, the AC in the GGG executes ANSI-41 authentication given the parameters received in the previous step, and the value of Kc (SSD-A) stored for that MS. The AC then invokes Authentication Request Return Result (IS41_authreq) towards the MSC/VLR to indicate successful ANSI-41 authentication.

[00179] In step 510, the GGG initiates the GSM1x authentication process by invoking GSM1x Authentication Requests using the IS41_SMDPP transport.

[00180] In step 511, the MSC forwards this SMS to the MS.

[00181] In step 512, the MS responds to the GSM1x authentication request by computing SRES and Kc using the GSM authentication method, and sending a response (GSM1x Auth Rsp) using IS-637 SMS transport.

[00182] In step 513, the MSC forwards the SMS to the GGG, and the GGG validates that the SRES in the GSM1x Auth Rsp matches the value received from the GSM HLR/AuC. This step completes the SSD update to the MS.

[00183] In step 514, upon the next system access by the MS, the MSC/VLR invokes Authentication Request (IS41_AUTHREQ) towards the GGG.

[00184] In step 515, the AC in the GGG executes ANSI-41 authentication given the parameters received in the previous step, and the value of Kc (SSD-A) stored for that MS. The AC then invokes Authentication Request Return Result (IS41_authreq) towards the MSC/VLR to indicate successful ANSI-41 authentication. The SSD parameter is also included to share SSD with the MSC/VLR.

Initial registration with SSD sharing

[00185] Figure 7 shows an initial registration scenario modified for SSD sharing in accordance with an embodiment. The information flow shown in Figure 7 is similar to the information flow shown in the flowchart of Figures 3a and 3b until step 619.

[00186] In step 601, the initial registration scenario begins when the MS performs a registration system access.

[00187] In step 602, the ANSI-41 MSC/VLR invokes Authentication Request (IS41_AUTHREQ) towards the HLR in the GGG (the HLR for the GSM1x MS). The relevant parameters in this AUTHREQ are MIN, ESN and COUNT. The GGG stores the value of ESN and compares the value of COUNT to the value in the database.

[00188] In step 603, the GGG looks up the MIN in its database to get the corresponding GSM IMSI and invokes the MAP_SEND_AUTHENTICATION_INFO towards the GSM HLR/AuC.

[00189] In step 604, the GGG invokes the Authentication Request Return Result (IS41_authreq) towards the MSC/VLR indicating successful authentication and starts a timer, TREG.

[00190] In step 605, upon receiving the IS41_authreq indicating successful authentication the MSC/VLR invokes Registration Notification (IS41_REGNOT) towards the HLR in the GGG.

[00191] In step 606, if the GGG receives the IS41_REGNOT before TREG expires (as in this scenario), then it responds with a Registration Notification Return Result (IS41_regnot) with a profile macro authorizing SMS only. SMS only is specified as follows:

[00192] SMS_OriginationRestriction = "allow all"

[00193] SMS_TerminationRestriction = "allow all"

[00194] OriginationIndicator = "single directory number" (e.g., plays announcement)

[00195] In step 607, upon receiving the IS41_regnot the MSC/VLR sends registration accept to the MS.

[00196] In step 608, the GGG receives the MAP_send_authentication_info from the GSM HLR/AuC containing one or more authentication triplets.

[00197] In step 609, after the GGG successfully sends the IS41_regnot to the MSC/VLR (6) and receives the MAP_send_authentication_info from the GSM HLR/AuC (8), it sends the GSM1x authentication request (GSM1x Auth Req) message using IS41_SMDPP transport.

[00198] In step 610, the MSC forwards this SMS to the MS.

[00199] In step 611, the MS responds to the GSM1x authentication request by computing SRES and Kc using the GSM authentication method and sending a response (GSM1x Auth Rsp) using IS-637 SMS transport.

[00200] In step 612, the MSC forwards the SMS to the GGG and the GGG validates that the SRES in the GSM1x Auth Rsp matches the value received from the GSM HLR/AuC.

[00201] In step 613, the GGG invokes MAP_UPDATE_LOC towards the GSM HLR to update the location of the MS.

[00202] In step 614, the GSM HLR invokes MAP_INSERT_SUB_DATA towards the GSM VLR in the GGG to send the subscriber profile.

[00203] In step 615, the GGG maps the GSM subscriber profile to an ANSI-41 subscriber profile and sends this ANSI-41 profile to the MSC/VLR by invoking Qualification Directive (IS41_QUALDIR).

[00204] In step 616, the MSC/VLR responds to the Qualification Directive of step 615.

[00205] In step 617, The GGG responds to the MAP_INSERT_SUB_DATA of step 614.

[00206] In step 618, the GSM HLR responds to the MAP_UPDATE_LOC of step 613.

[00207] In step 619, upon the next system access by the MS the following steps occur:

[00208] In step 620, the MSC/VLR VLR invokes Authentication Request (IS41_AUTHREQ) towards the GGG.

[00209] In step 621, the AC in the GGG executes ANSI-41 authentication given the parameters received in the previous step and the value of Kc (SSD-A) stored for that MS. The AC then invokes Authentication Request Return Result (IS41_authreq) towards the MSC/VLR to indicate successful ANSI-41 authentication. The SSD parameter is also included to share SSD with the MSC/VLR.

Registration at new MSC/VLR with SSD sharing

[00210] Figure 8 shows the information flow for a successful registration with a new MSC/VLR when SSD sharing is allowed in accordance with an embodiment.

[00211] In step 715, upon the next system access by the MS the following steps occur:

[00212] In step 716, the MSC/VLR VLR invokes Authentication Request (IS41_AUTHREQ) towards the GGG.

[00213] In step 717, the AC in the GGG executes ANSI-41 authentication given the parameters received in the previous step and the value of Kc (SSD-A) stored for that MS. The AC then invokes Authentication Request Return Result (IS41_authreq) towards the MSC/VLR to indicate successful ANSI-41 authentication. The SSD parameter is also included to share SSD with the MSC/VLR.

Ciphering

[00214] GSM Ciphering is based on successful GSM Authentication. The RAND value sent to the MS by the MSN for authentication is also used in the creation of the GSM Kc. The RAND value is passed to the SIM to create a Kc value. In an embodiment, a GSM A8 algorithm, which is known in the art, is used to create the Kc value. The SIM returns Kc to the MS for bulk encryption (using A8) in a GSM network. A3 and A8 are authentication and key generation functions.

Outline of Authentication Procedure

[00215] Figure 9 shows an outline of an authentication procedure for a GSM mobile station in accordance with an embodiment. Figure 9 is an outline of the authentication process that is used by a GSM mobile station.

[00216] An MSN 902 sends an authentication request 904 with a random number RAND to an MS 906. The RAND is sent by the MS 906 to the GSM SIM card 908. Note the RAND of Figure 9 is the same as GSM_RAND shown in Figure 4.

[00217] The MS 906 interfaces with a GSM SIM card 908. In an embodiment, the GSM SIM card is removable. Alternatively, the GSM card is integrated into the MS 906. In an embodiment, the GSM SIM 908 uses a GSM authentication algorithm to calculate SRES, which is sent to the MSN 902.

[00218] In an embodiment, the MS 906 responds to the authentication request 904 by computing SRES and Kc using the GSM authentication method, and sending an authentication response with SRES to the MSN 902.

[00219] The MSN 902 verifies the SRES returned from the GSM SIM 908 to the MSN 902. The MSN verifies that the SRES returned by the GSM SIM card 908 matches the SRES provided to it by the GSM AuC (not shown).

Key Generation

[00220] Figure 10 describes GSM key generation with a GSM MS in a GSM network. Figure 11 describes CDMA key generation with a CDMA MS in a CDMA network.

[00221] In accordance with an embodiment, the system seamlessly integrates a CDMA RAN with a GSM Core network. This is achieved using a GSM MSN that couples the CDMA RAN to the GSM Core network. The ciphering design combines both GSM and CDMA

Key Generation algorithms. In an embodiment, the system uses a spreading sequence such as a PLC to scramble voice traffic. In an embodiment, GSM key generation uses A5/1 - a Ciphering algorithm. In an embodiment, GSM key generation uses A5/2.

[00222] In an embodiment, the system combines the GSM key generation of Figure 10 with the CDMA key generation of Figure 11 such that a mobile station with a subscription in a GSM network, i.e., a mobile station that has access to Ki from the GSM network, can roam in a CDMA network and be authenticated according to the GSM subscription and messages sent and received by the mobile station can be encrypted. Thus, the mobile station with a GSM SIM works in a CDMA network seamlessly.

[00223] In accordance with an embodiment, Figure 10 describes a GSM Key Generation process, which is used for GSM authentication and privacy. Figure 10 defines how GSM authentication and cryptography work in a GSM context.

[00224] RAND 1002 and Ki 1004 are inputs to two algorithms, A3 1006 and A8 1008.. These two elements generate two other elements, SRES 1010 and Kc 1012. SRES 1010 is an authentication parameter. During the authentication process, the network gets a response, which has SRES in it, back from either the SIM or authentication center. The network is authenticates the mobile station based on SRES.

[00225] GSM Privacy means encryption of voice packets. From the voice traffic 1014, every voice frame gets encrypted to prevent other devices from decoding the voice frames. Other devices cannot decode the voice frames because they do not have access to Kc.

[00226] A8 1008 generates Kc, which is a ciphering key. Kc is used to do voice ciphering. Kc and the voice traffic element 1014, which provides a number of bits for speech encoding are combined together using algorithms A5/1 or A5/2 1016. The A5/1 or A5/2 algorithms 1016 enable GSM ciphering for GSM privacy.

[00227] Figure 11 shows CDMA Key Generation in accordance with an embodiment.

[00228] The CDMA Authentication process is turned off. However, the GSM MSN and MS will generate a voice privacy mask (VPM) for voice privacy (VP). The GSM MS and MSN will generate an Enhanced Cellular Message Encryption Algorithm (ECMEA) Key for Signaling Privacy.

[00229] The MSN and MS will replace the following elements in the process of calculating the VPM for VP, and the ECMEA Key for Signaling Privacy.

[00230] SSD-A is replaced with Kc.

[00231] SSD-B is replaced with Kc.

[00232] ESN is replaced with IMSI.

[00233] Both the network and the mobile station have an A-key 1102, which is never sent over the network. ESN 1104, A-Key 1102, and RAND 1106 are inputs to a CAVE algorithm 1108. This RAND 1106 of Figure 11 is the same as the RAND of Figure 4. The CAVE algorithm 1108 produces SSD 1110. The SSD 1110 is 128 bits, which is divided into two parts, SSD-A 1112 and SSD-B 1114. SSD-A 1112 and SSD-B 1114 become inputs to two other rungs of a CAVE algorithm 1116, 1118. One of the rungs 1116 is used to calculate authentication information, AUTHR 1120. These authentication bits are a sequence of bits that are sent with every access, so the network is capable of determining that no other device except the mobile that has the shared secret data SSD could have generated the authentication AUTHR. That is how the network is able to determine whether the mobile station is authenticated. Similarly, the network always sends a RAND, which enables the mobile station to determine the network. The concern for authentication is to make sure the network is communicating with the correct mobile station.

[00234] SSD-B 1114 goes to another instantiation of the CAVE algorithm 1118. Other inputs to the CAVE algorithm 1118 include ESN 1114, authentication data such as MIN or last dialed digits 1122, and output of CAVE algorithm 1116 that was executed using SSD-A. The CAVE algorithm 1118 processes these inputs to produce VPMASK 1124 and CMEAkey 1126. VPMASK and CMEAkey are used encrypt CDMA packets. Just as GSM key generation provided Kc and algorithms A5/1 and A5/2 were executed using Kc, CDMA key generation provides SSD-B and a CAVE algorithm is executed using SSD-B. In both cases, ciphers are generated for encryption.

[00235] In an embodiment, the system combines GSM key generation of Figure 10 with CDMA key generation of Figure 11. A random number is sent to a mobile station with a GSM SIM just like in Figure 10 and the mobile station generates Kc. Kc is then substituted for the SSD-A and SSD-B in the CDMA key generation of Figure 11. Then, the mobile station performs exactly as shown in the CDMA key generation of Figure 11.

[00236] Thus, in a hybrid mode of operation, i.e., a mobile station with a GSM SIM roaming into a CDMA network, the mobile station generates Kc and SRES using a random number. Once Kc is created, Kc is substituted for SSD-A and SSD-B, which enables both the network and mobile station to have valid authentication data & encryption.

Message Flow During Registration

[00237] Figures 12-14 describe a message flow in accordance with an embodiment for a hybrid authentication mode, i.e., a mobile station having a GSM SIM roaming in a CDMA network. MSN is at the same level as an MSC in a CDMA network. In another embodiment, the same procedure is followed in a network with a GGG. In the GGG configuration, the network has a CDMA MSC instead of the MSN and the network includes a GGG just as shown in Figures 6-8.

[00238] Figure 12 shows a message flow during registration in accordance with an embodiment. Figure 12 describes the message flow for the first time the mobile station is authenticated.

[00239] Figure 12 assumes the mobile station had been just switched on. The mobile station sends a registration message 1202, which gets sent to the MSN as part of a Location Update Request 1204. The registration message gets converted to a Location Update Request on the interface between the BTS/BSC and the MSN. The interface between the BTS/BSC and MSN is called the A-interface, which is defined by the CDMA2000 standard.

[00240] After the Location Update Request is received by the MSN, the MSN sends a MAP_SEND_AUTHENTICATION Info 1206 to the GSM HLR/AuC 1206. The MSN sends the MAP_SEND_AUTHENTICATION Info 1206 to the GSM HLR/AuC 1206 to obtain authentication information for the mobile station. The MSN obtains SRES, a random number, Kc, and other authentication parameters as required in a MAP_SEND AUTHENTICATION Response 1208 from the GSM HLR/AuC. For subsequent authentications, the MSN can obtain different authentication parameters.

[00241] Triplets (SRES, random number, and Kc) are stored in the MSN. The MSN then sends a GSM authentication request 1210 to the BTS/BSC. SMS is used to encapsulate the random number as described earlier. The random number travels through a data burst message, Auth Request DataBurst 1212, to the mobile station. The mobile station responds to the Auth Request DataBurst 1212 with a Auth Response DataBurst 1214.

[00242] The random number is sent to the SIM by the mobile station. The SIM then returns the SRES and calculates the Kc. SRES is returned back to the MSN in the Authentication Response 1216. The MSN then can compare the SRES received from the AuC with the SRES the mobile sends and if the two SRES match, then the MSN determines that the mobile station is authentic and the mobile station is authenticated.

[00243] The MSN updates the GSM HLR with an Update Location Request 1218. The GSM HLR responds to the Update Location Request 1218 with an Update Location Response 1220. After receiving the Update Location Response 1220, the MSN sends a Location Update Accept 1222 to the BTS/BSC. The BTS/BSC sends a Registration Accepted Order to the mobile station and the mobile station is allowed to use the GSM network.

[00244] At the end of the message flow of Figure 12, the mobile station has a Kc, which is the same as the Kc the AuC sends to the MSN. Both the MSN and the mobile station have the same Kc and both are ready are encryption. Figures 13 and 14 are the call flows that enable encryption.

[00245] In an embodiment, GSM Authentication is performed immediately after Registration to provide the optimum privacy. In an embodiment, Voice and Signaling Privacy is requested in the Page Response for a mobile terminated (MT) Call, or the Origination Message for a mobile originated (MO) Call after the MS has passed the GSM Authorization process.

[00246] The next two cases exist if a phone is powered on and a call is made or received before Registration is complete.

Message Flow During Mobile Originated Call

[00247] Figure 13 shows the message flow during an MO call in accordance with an embodiment. The MSN shall send the VPM and ECMEA Key to the BTS during call setup in the PRIVACY_MODE_REQUEST message of the ENCRYPTION_INFORMATION field.

[00248] Figure 13 can be divided into two parts. The part above the Authentication Procedure is the CDMA call set up. The mobile sends an origination 1302 and the BTS/BSC sends an acknowledgment order 1304, which indicates that the BTS/BSC has received the origination message. The acknowledgment order 1304 is needed since an origination message may not be sent reliably.

[00249] The BTS/BSC sends a a CM_Service_Request to the MSN 1306 to set up a call. As a result of this request, the MSN sends an Assignment Request 1308 to the BTS/BSC to get a channel assigned to the mobile. The BTS/BSC sends a CH Assign 1310 to the mobile station.

[00250] The mobile station sends a traffic channel (TCH) preamble 1312 to the BTS/BSC. The TCH preamble 1312 means the mobile station is making a noise. The BTS/BSC

listens to the mobile station and attempts to acquire the mobile station. As soon as the BTS/BSC acquires the mobile station, the BTS/BSC sends a forward (FW) Ack Order 1314 to the mobile station. The FW Ack Order 1314 indicates the BTS/BSC has received the TCH preamble 1312.

[00251] A Service Connect 1316 is sent from the BTS/BSC to the mobile station. The Service Connect from the BTS/BSC indicates to the mobile station that the mobile station is on service now and is ready. The mobile station acknowledges the Service Connect with a Service Connect Complete 1318 to the BTS/BSC, which then translates to an Assignment Complete 1320 from the BTS/BSC to the MSN. At this point, the MSN has a traffic channel to the mobile.

[00252] IAM 1322 and ACM 1324 are SS7 signaling to the telephone network setting up a link on the other side with the PSTN. The mobile station is making a call. IAM message makes the called device "ring." ACM is the completion of the SS7 call setup.

[00253] After the traffic channel is set up, a GSM authentication procedure can be optionally performed. The optional GSM authentication procedure can run on overhead channels or traffic channels. For a mobile originated call, the MSN can decide to run the authentication procedure optionally. But even if the MSN does not run the authentication procedure, then the last Kc that the mobile station generated is the same Kc as the MSN Kc. The Kc only changes when the GSM authentication procedure is performed.

[00254] Once a user answers at the other end of a call, the PSTN sends an ANM 1326 to the MSN. ANM 1326 is an answer message per SS7 signaling, that the called device has been picked up. After the user answers at the other end of a call, the MSN can decide to turn on privacy mode 1328 that indicates to the BTS/BSC to start encrypting and in the Privacy Mode message, is a calculated long code mask. The MSN indicates to the BTS to use the VPM Mask and CMEA key and it is sending these keys in the Privacy Mode message.

[00255] The VPM Mask and CMEA key are used as described in the CDMA2000 standard. They are used to encrypt voice packets. In the Privacy Mode message 1328, the MSN indicates to the mobile station to start encrypting and the mobile acknowledges responds with a Request Privacy Long Code Transition Response 1332..

[00256] The BTS/BSC sends the MS a Request Privacy Long Code Transition Order 1330 and the mobile station responds with a Request Privacy Long Code Transition Response 1332.

[00257] After receiving the Request Privacy Long Code Transition Response 1332, the BTS/BSC sends a Privacy Mode Complete 1334 to the MSN. After the Privacy Mode is complete, the mobile station is in a scrambled talk state meaning that voice frames are being encrypted.

Message Flow During Mobile Terminated Call

[00258] Figure 14 shows the message flow during a mobile terminated (MT) call in accordance with an embodiment. The MSN shall send the VPM and ECMEA Key to the BTS during call setup in the PRIVACY_MODE_REQUEST message of the ENCRYPTION_INFORMATION field.

[00259] Figure 14 is an example of Privacy Mode when a call is originated on the PSTN side. The call could involve another mobile station calling this mobile station. The messages between MSN and PSTN are regularly defined as SS7 messages that are used to send origination and termination message to the PSTN.

[00260] IAM 1402 is a request indicating to the MSN that a call is being initiated to the mobile station. In response to the IAM, the MSN pages the mobile because the mobile is previously registered as defined by Figure 12. The MSN sends a Paging Request 1404 to the BTS/BSC. At this point, the mobile already has a Kc because it was previously authenticated using GSM authentication procedure.

[00261] Upon receiving a Paging Request from the MSN, the BTS/BSC sends a General Page 1406 to the mobile station. The mobile station responds to the page with a Page Response 1408 sent to the BTS/BSC. The BTS/BSC sends a Page Response 1410 to the MSN. Once the Page Response 1410 is received by the MSN, the MSN knows the mobile is there and is ready to receive a call. The MSN then sends an Assignment Request 1412 to the BTS/BSC. The Assignment Request 1412 indicates to the BTS/BSC to set up a channel for the mobile and the BTS/BSC assigns a channel to the mobile and sends a channel assign 1414 to the mobile station.

[00262] The mobile station sends a TCH Preamble 1416 to the BTS/BSC. The TCH Preamble 1416 indicates the mobile is making some noise on the forward channel so that BTS/BSC can acquire the mobile station. The BTS/BSC sends an FW Ack Order 1418 to the mobile station after receiving the TCH Preamble.

[00263] Once the BTS/BSC acquires the mobile station, there is a Service Connect 1420 and a Service Connect Complete 1422. The BTS/BSC sends a Service Connect 1420 to the

mobile station and the mobile station responds to the Service Connect 1420 with a Service Connect Complete 1422.

[00264] The BTS/BSC sends an Alert with Info 1424 to the mobile station. The Alert with Info is a request for the mobile station to ring. After the mobile station starts ringing, an Assignment Complete 1426 is sent from the BTS/BSC to the MSN. The Assignment Complete indicates to the MSN that the mobile station is ringing and a channel has been assigned to the mobile station. An ACM 1428 is sent from the MSN to the PSTN indicating to the PSTN the mobile station is ringing.

[00265] At some point, a user picks up the called mobile station and a Connect Order 1430 is sent from the mobile station to the BTS/BSC. Then, the BTS/BSC sends a Connect 1432 to the MSN.

[00266] Once the connection has been established, the GSM authentication procedure can be optionally run. It is optional when to run the GSM authentication procedure, therefore an authentication policy can dictate that the authentication procedure be run once every five calls or once every ten calls for example. The AuC indicates the authentication policy to the MSN, and then the MSN can follow that policy.

[00267] When the Authentication procedure is run, new values of Kc are determined, which would be synchronized as previously described. The privacy mode request 1434, request privacy long code transition order 1436, request privacy long code transition response 1438, privacy mode complete 1440, and ANM 1442 operate as described in Figure 13. After the ANM 1442 is sent from the MSN to the PSTN, the MSN starts the call, which runs in Scramble mode. ANM is the answer message as before.

[00268] Note that in a GSM network, the Authentication center tells the GSM MSC, when the GSM MSC should do authentication. In a CDMA network there is no such mapping such that the AuC indicates to the MSC when to do authentication. However, for a mixed mobile station, i.e., a mobile station with a GSM SIM roaming in a CDMA network, the GSM authentication procedure can be run whenever the MSN needs to run it, i.e., according to authentication policies of the MSN. Thus, the MSN can implement the policies set by the AuC.

[00269] While the particular CIPHERING BETWEEN A CDMA NETWORK AND A GSM NETWORK as herein shown and described in detail is fully capable of attaining the above-described objects of the invention, it is to be understood that it is the presently preferred embodiment of the present invention and is thus representative of the subject

matter which is broadly contemplated by the present invention, that the scope of the present invention fully encompasses other embodiments which may become obvious to those skilled in the art, and that the scope of the present invention is accordingly to be limited by nothing other than the appended claims, in which reference to an element in the singular is not intended to mean "one and only one" unless explicitly so stated, but rather "one or more". All structural and functional equivalents to the elements of the above-described preferred embodiment that are known or later come to be known to those of ordinary skill in the art are expressly incorporated herein by reference and are intended to be encompassed by the present claims. Moreover, it is not necessary for a device or method to address each and every problem sought to be solved by the present invention, for it to be encompassed by the present claims. Furthermore, no element, component, or method step in the present disclosure is intended to be dedicated to the public regardless of whether the element, component, or method step is explicitly recited in the claims. No claim element herein is to be construed under the provisions of 35 U.S.C. §112, sixth paragraph, unless the element is expressly recited using the phrase "means for" or, in the case of a method claim, the element is recited as a "step" instead of an "act".

[00270] Method steps can be interchanged without departing from the scope of the invention.

What is claimed is: